EXHIBIT 8

PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td>A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:</td><td>Trend Micro Apex Central includes <i>a computer program product embodied on a non-transitory computer readable medium</i> (e.g., Trend Micro threat detection and/or security appliances, etc.), <i>the computer program product comprising:</i>

“<b>About the Web Console</b>

The Apex Central web console provides centralized management, monitoring, and security visibility for all endpoints and users protected by Trend Micro products registered to the Apex Central server. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications. <u>The web console lets you administer the Apex Central network from any machine using a compatible web browser</u>.

Apex Central supports the following web browsers:<ul><li>Microsoft Internet Explorer™ 11</li><li>Microsoft Edge™</li><li>Google Chrome™</li></ul><b>Web Console Requirements</b>

<table><tr><th>Resource</th><th>Requirement</th></tr><tr><td>Processor</td><td>300 MHz Intel™ Pentium™ processor or equivalent</td></tr><tr><td>RAM</td><td>128 MB minimum</td></tr><tr><td>Available disk space</td><td>30 MB minimum</td></tr></table></td></tr>
</table>

EXHIBIT 8

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Browser</td><td>Microsoft Internet Explorer™ 11, Microsoft Edge™, or Google Chrome™
Important: When using Internet Explorer to access the Apex Central web console, turn off Compatibility View.</td></tr>
</table>
<p><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 2-2 to 2-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</p>
<p>"<b>Attack Discovery Detection Information</b></p>
<p>Provides general information about threats detected by Attack Discovery</p>
<table>
<tr><th>Data</th><th>Description</th></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Endpoint</td><td>The name of the endpoint</td></tr>
<tr><td>Product</td><td>The name of the managed product or service</td></tr>
<tr><td>Managing Server Entity</td><td>The display name of the managed product server in Apex Central to which the endpoint reports</td></tr>
<tr><td>Product Version</td><td>The version of the managed product</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Risk Level</td><td>The risk level assigned by Attack Discovery</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Pattern Version</td><td>The Attack Discovery pattern number for the detection type</td></tr>
<tr><td>Rule ID</td><td>The serial number of the detection rule</td></tr>
<tr><td>Rule Name</td><td>The rules which specify behaviors to be detected by Attack Discovery</td></tr>
<tr><td>Related Objects</td><td>The number of detections

Click the count to view additional details.

For more information, see Detailed Attack Discovery Detection Information on page B-11.</td></tr>
<tr><td>Generated (Local Time)</td><td>The time in the agent's local timezone when Attack Discovery detected the threat

The time is displayed with the UTC offset.</td></tr>
<tr><td>Instance ID</td><td>The detection ID assigned to the event

Entries having the same instance ID belong under the same event.</td></tr>
<tr><td>Tactics</td><td>The MITRE ATT&CK™ tactic(s) detected

For more information, see https://attack.mitre.org/tactics/enterprise/.</td></tr>
<tr><td>Techniques</td><td>The MITRE ATT&CK™ technique(s) detected</td></tr>
</table>
</td></tr>
</table>

Claim 14 Elements	Applicability
	For more information, see https://attack.mitre.org/techniques/enterprise/. *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page B-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**Threat Encyclopedia** Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities. Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about: • Malware and malicious mobile code currently active or "in the wild" • Correlated threat information pages to form a complete web attack story • Internet threat advisories about targeted attacks and security threats • Web attack and online trend information • Weekly malware reports" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 25-2 to 25-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) **Note**: As set forth below, managed product and child server information is equivalent to memory on the at least one device. "**Understanding the Apex Central Database**

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

Claim 14 Elements	Applicability
	Apex Central uses the Microsoft SQL Server database (db_ApexCentral.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. The Apex Central server establishes the database connection using a System DSN ODBC connection. The Apex Central installation generates this connection as well as the ID and password used to access db_ApexCentral.mdf. The default ID is sa. Apex Central encrypts the password. To maximize the SQL server security, configure any SQL account used to manage db_ApexCentral with the following minimum permissions: • dbcreator for the server role • db_owner role for db_ApexCentral Logs from managed products contribute to database expansion. Managed products send various log types to Apex Central." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 23-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
code for: accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that	Trend Micro Apex Central includes *code for: accessing at least one data structure* (e.g., a repository of a smaller "sub-set" of actual vulnerabilities relevant to a particular operating system/application/version thereof, etc.) *identifying a plurality of mitigation techniques (e.g., threat analysis and/or outbreak control, etc.) that mitigate effects of attacks* (e.g., ransomware, known advanced persistent threat, social engineering attack, vulnerability attack, lateral movement, suspicious objects, and/or c&c callback, etc.) *that take advantage of vulnerabilities* (e.g., possible vulnerabilities that are relevant to the identified at least one

Claim 14 Elements	Applicability
take advantage of vulnerabilities, where: each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and	operating system, etc.)*, where: each mitigation technique (e.g., threat analysis and/or outbreak control, etc.) is capable of mitigating an effect of an attack* (e.g., ransomware, known advanced persistent threat, social engineering attack, vulnerability attack, lateral movement, suspicious objects, and/or c&c callback, etc.) *that takes advantage of a corresponding vulnerability* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.)*, and* "**Vulnerability attack** Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems." *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "Procedure 1. Go to **Administration > Security Agent Download**. 2. Select the operating system. • **Windows 64-bit**: Select to create a 64-bit MSI installation package for Apex One Security Agents • **Windows 32-bit**: Select to create a 32-bit MSI installation package for Apex One Security Agents • **Mac OS**: Select to create a ZIP installation package for Apex One (Mac) Security Agents" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 9-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "**About Apex Central**

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>Trend Micro Apex Central™ is a web-based console that provides centralized management for Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Apex Central web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Apex Central enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. Apex Central allows both manual and pre-scheduled updates, and allows the configuration and administration of products as groups or as individuals for added flexibility."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 1-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
<table><tr><th>Consideration</th><th>Effect</th></tr><tr><td>Deployment planning</td><td>Apex Central deploys update components (for example, virus pattern files, <b>scan</b> engines, anti-spam rules, <b>program updates</b>) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr></table><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>

Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with <b><i>recommended Intrusion Prevention</i></b> rules</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>based on your network performance and security priorities.</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"<b>Intrusion Prevention Rules</b>

The <b>Intrusion Prevention Rules</b> screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"...
5. In the Certified Safe Software List section, configure the following:
• <b>Enable the local Certified Safe Software List</b>: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.
</td></tr>
</table>

Claim 14 Elements	Applicability

- **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

  Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service."

https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

"The Threat Type column displays the following threat types.

Threat Type	Description
Ransomware	Malware that prevents or limits users from accessing their system unless a ransom is paid
Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;</td><td>
Trend Micro Apex Central includes <i>each mitigation technique</i> (e.g., threat analysis and/or outbreak control, etc.<i>) has a mitigation type including at least one of a patch, a policy setting, or a configuration option</i> (e.g., virtual patches, policy, firewall configuration settings, etc.)<i>;</i>
<table>
<tr><th>Consideration</th><th>Effect</th></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Deployment planning</td><td>Apex Central deploys <b>update components</b> (for example, virus pattern files, scan engines, anti-spam rules, <b>program updates</b>) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system
…
Table 1. Product Status Information Data View
<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table><tr><td></td><td>product server or Security Agent endpoint</td></tr></table>

Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

"…

5. In the Certified Safe Software List section, configure the following:

- **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

  - **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

    Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.

6. In the Exception section, manage the Exception Template List that applies to this policy only.

   The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.

   For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).

7. Click **Save**."
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<p>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</p>
<p>“<b>Detailed Firewall Violation Information</b></p>
<p>Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations”</p>
<table>
<tr><th>Section</th><th>Settings</th></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Product Entity/Endpoint</td><td>Depending on the related source:<ul><li>The display name of the managed product server in Apex Central</li><li>The name or IP address of the endpoint Product</li></ul></td></tr>
<tr><td>Product</td><td>The name of the managed product or service
Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network
Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
<tr><td>Protocol</td><td>The protocol the intrusion uses
Example: HTTP, SMTP, FTP</td></tr>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product
Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections</td></tr>
</table>
</td></tr>
</table>

Claim 14 Elements	Applicability

	Example: A managed product detects 10 violation instances of the same type on one computer Detections = 10

Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

Feature	**Description**
...	...
Vulnerability Protection Integration	Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with ***recommended Intrusion Prevention*** rules based on your network performance and security priorities.
...	...

https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"**Intrusion Prevention Rules**

The **Intrusion Prevention Rules** screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.
<ul>
<li>To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.</li>
<li>To sort the list of Intrusion Prevention Rules by column data, click a column heading.</li>
<li>To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."</li>
</ul>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"The Threat Type column displays the following threat types.
<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>code for:

receiving information in connection with at least one of a plurality of devices; and</td><td>Trend Micro Apex Central includes <i>code for: receiving information</i> (e.g., activity at a device, etc.) <i>in connection with at least one of a plurality of devices</i> (e.g., managed products and endpoints, etc.)<i>; and</i>

"<b>Component Updates</b></td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>The Apex Central server hosts component files that the managed products use to keep your network protected from the latest security threats.

Keep the components up-to-date by running manual or scheduled updates. Apex Central allows you to perform the following tasks:
• Download the latest component versions from an update source
• Deploy updated components to managed products

"<b>Update Source</b>

Configure the Apex Central server to download components from the Trend Micro ActiveUpdate server or other update sources. You can specify other update sources if the Apex Central server is unable to connect to the Trend Micro ActiveUpdate server directly or if you host an update server in your network.

By default, Apex Central uses a more secure HTTPS connection method to download components from the Trend Micro ActiveUpdate server.

To access other update sources, Apex Central supports Remote UNC authentication, which uses a user account from the update source server to share a folder for Apex Central to download updates."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 11-2 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

<table><tr><th>Consideration</th><th>Effect</th></tr><tr><td>Deployment planning</td><td>Apex Central deploys update components (for example, <b>virus</b> pattern files, <b>scan</b> engines, anti-spam rules, <b>program updates</b>)</td></tr></table></td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View
<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with <b><i>recommended Intrusion Prevention</i></b> rules based on your network performance and security priorities.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"<b>Intrusion Prevention Rules</b>

The <b>Intrusion Prevention Rules</b> screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

Claim 14 Elements	Applicability
	Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf) "... 5. In the Certified Safe Software List section, configure the following: - **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern. - **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**."

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)</td></tr>
<tr><td>identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information;</td><td>Trend Micro Apex Central includes <i>identifying an attack</i> (e.g., ransomware, known advanced persistent threat, social engineering attack, vulnerability attack, lateral movement, suspicious objects, and/or c&c callback, etc.) <i>on the at least one device</i> (e.g., managed products and endpoints, etc.) <i>that takes advantage of at least one of the vulnerabilities</i> (e.g., possible vulnerabilities that are relevant to the identified at least one operating system, etc.), <i>based on the information</i> (e.g., activity at a device, etc.)<i>;</i>
<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td>Apex Central deploys <b>update components</b> (for example, virus pattern files, scan engines, anti-spam rules, <b>program updates</b>) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system
…</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
Table 1. Product Status Information Data View
<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

"…
5. In the Certified Safe Software List section, configure the following:
• **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

• **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.

Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service.
</td></tr>
</table>

Claim 14 Elements	Applicability

6. In the Exception section, manage the Exception Template List that applies to this policy only.

    The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List.

    For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3).

7. Click **Save**."

https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added)

"**Detailed Firewall Violation Information**

Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations"

Section	Settings
Received	The date and time Apex Central received the data from the managed product
Generated	The date and time the managed product generated the data
Product Entity/Endpoint	Depending on the related source:

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>• The display name of the managed product server in Apex Central
• The name or IP address of the endpoint Product</td></tr>
<tr><td>Product</td><td>The name of the managed product or service
Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection
Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network
Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
<tr><td>Protocol</td><td>The protocol the intrusion uses
Example: HTTP, SMTP, FTP</td></tr>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product

Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections

Example: A managed product detects 10 violation instances of the same type on one computer

Detections = 10</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with ***recommended Intrusion Prevention*** rules based on your network performance and security priorities.</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"<b>Intrusion Prevention Rules</b>

The <b>Intrusion Prevention Rules</b> screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"The Threat Type column displays the following threat types.

<table><tr><th>Threat Type</th><th>Description</th></tr><tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr></table></td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro’s Apex Central

Claim 14 Elements	Applicability	
	Known Advanced Persistent Threat (APT)	Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents
	Social engineering attack	Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file
	Vulnerability attack	Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems
	Lateral movement	Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system
	Unknown threats	Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer
	C&C callback	Attempts to communicate with a command-and-control (C&C) server to

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>code for:

automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, for mitigating an effect of the attack on the at least one device that takes advantage of the at least one vulnerability;</td><td>
Trend Micro Apex Central includes *code for: automatically applying at least two of the plurality of mitigation techniques (e.g., threat analysis and/or outbreak control, etc.) including at least one first mitigation technique of a first mitigation type* (e.g., firewall configuration, etc.) *and at least one second mitigation technique of a second mitigation type* (e.g., intrusion detection, etc.) *to the at least one device* (e.g., managed products and endpoints, etc.), *for mitigating an effect of the attack* (e.g., ransomware, known advanced persistent threat, social engineering attack, vulnerability attack, lateral movement, suspicious objects, and/or c&c callback, etc.) *on the at least one device* (e.g., managed products and endpoints, etc.) *that takes advantage of the at least one vulnerability* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.)*;*
<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td>Apex Central deploys **update components** (for example, virus pattern files, scan engines, anti-spam rules, **program updates**) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system
…
Table 1. Product Status Information Data View
<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>
Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center
"…
5. In the Certified Safe Software List section, configure the following:
• **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.
• **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern.
</td></tr>
</table>

Claim 14 Elements	Applicability
	Important: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added) "**Detailed Firewall Violation Information** Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations"

Section	Settings
Received	The date and time Apex Central received the data from the

Patent No. 9,100,431, Claim 14: Trend Micro’s Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>managed product</td></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Product Entity/Endpoint</td><td>Depending on the related source:
• The display name of the managed product server in Apex Central
• The name or IP address of the endpoint Product</td></tr>
<tr><td>Product</td><td>The name of the managed product or service
Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection
Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network
Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
<tr><td>Protocol</td><td>The protocol the intrusion uses
Example: HTTP, SMTP, FTP</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product
Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections
Example: A managed product detects 10 violation instances of the same type on one computer
Detections = 10</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>patches become available. Trend Micro provides protected endpoints with <b><i>recommended Intrusion Prevention</i></b> rules based on your network performance and security priorities.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"<b>Intrusion Prevention Rules</b>

The <b>Intrusion Prevention Rules</b> screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"The Threat Type column displays the following threat types.
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email messages) with the "high" risk level, as detected by Deep Discovery Inspector,</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>endpoint security products, or other products with Virtual Analyzer</td></tr>
<tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
<tr><td>wherein the computer program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability;</td><td>
Trend Micro Apex Central includes code *wherein the computer program product is operable such that the effect of the attack* (e.g., ransomware, known advanced persistent threat, social engineering attack, vulnerability attack, lateral movement, suspicious objects, and/or c&c callback, etc.) *is mitigated by preventing the attack from taking advantage* (e.g., exploiting, etc.) *of the at least one vulnerability* (e.g., the subset of the possible vulnerabilities that is relevant to the identified at least one operating system, etc.)*;*
<table>
<tr><th>Consideration</th><th>Effect</th></tr>
<tr><td>Deployment planning</td><td>Apex Central deploys **update components** (for example, virus pattern files, scan engines, anti-spam rules, **program updates**) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.</td></tr>
</table>
Trend Micro Apex Central Administrator's Guide, Version: 2019, Page 10-13 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>

"Provides detailed information about managed products registered to the Apex Central server, such as the managed product version and build number, and the managed product server operating system

…

Table 1. Product Status Information Data View

<table>
<tr><td>Operating System</td><td>The operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Version</td><td>The version of the operating system on the managed product server or Security Agent endpoint</td></tr>
<tr><td>OS Service Pack</td><td>The service pack number of the operating system on the managed product server or Security Agent endpoint</td></tr>
</table>

Trend Micro Apex Central 2019 Online Help / Enterprise / Online Help Center

"…

5. In the Certified Safe Software List section, configure the following:

- **Enable the local Certified Safe Software List**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the local pattern.

</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

Claim 14 Elements	Applicability
	- **Enable the global Certified Safe Software List (Internet access required)**: Select to allow network traffic to applications that Trend Micro has verified to be safe, using the dynamically updated, cloud-based pattern. **Important**: Querying the global Certified Safe Software List requires that you enable both the Unauthorized Change Prevention Service and the Certified Safe Software Service. 6. In the Exception section, manage the Exception Template List that applies to this policy only. ***The Apex One Firewall automatically populates the Exceptions List with the Exception Template List entries. If you add, modify, or delete any exception in the policy Exceptions List, the changes only apply to the current policy and not the Exception Template List***. For more information about adding exceptions, see Adding a Firewall Policy Exception (follow the instructions from step 3). 7. Click **Save**." https://docs.trendmicro.com/en-us/enterprise/apex-one-as-a-service-online-help/officescan-agent-sca/using-the-officescan/firewall-policies/adding-a-firewall-po.aspx (emphasis added) "**Detailed Firewall Violation Information** Provides specific firewall configuration information on your network, such as the managed product that detected the violation, the source and destination of the transmission, and the total number of firewall violations"

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><th>Section</th><th>Settings</th></tr>
<tr><td>Received</td><td>The date and time Apex Central received the data from the managed product</td></tr>
<tr><td>Generated</td><td>The date and time the managed product generated the data</td></tr>
<tr><td>Product Entity/Endpoint</td><td>Depending on the related source:
• The display name of the managed product server in Apex Central
• The name or IP address of the endpoint Product</td></tr>
<tr><td>Product</td><td>The name of the managed product or service
Example: Apex One, ScanMail for Microsoft Exchange</td></tr>
<tr><td>Event Type</td><td>The type of event that triggered the detection
Example: intrusion, policy violation</td></tr>
<tr><td>Risk Level</td><td>The Trend Micro assessment of risk to your network
Example: High security, low security, medium security</td></tr>
<tr><td>Traffic/Connection</td><td>The direction of the transmission</td></tr>
<tr><td>Protocol</td><td>The protocol the intrusion uses</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Example: HTTP, SMTP, FTP</td></tr>
<tr><td>Source IP</td><td>The source IP address of the detected threat</td></tr>
<tr><td>Endpoint Port</td><td>The port number of the endpoint under attack</td></tr>
<tr><td>Endpoint IP</td><td>The IP address of the endpoint</td></tr>
<tr><td>Target Application</td><td>The application the intrusion targeted</td></tr>
<tr><td>Description</td><td>The detailed description of the incident by Trend Micro</td></tr>
<tr><td>Action</td><td>The action taken by the managed product

Example: file cleaned, file quarantined, file passed</td></tr>
<tr><td>Detections</td><td>The total number of detections

Example: A managed product detects 10 violation instances of the same type on one computer

Detections = 10</td></tr>
</table>
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page B-51 to B-52 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>...</td><td>...</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
<table>
<tr><td>Vulnerability Protection Integration</td><td>Integration with Vulnerability Protection protects Apex One users by automating the application of virtual patches before official patches become available. Trend Micro provides protected endpoints with <b><i>recommended Intrusion Prevention</i></b> rules based on your network performance and security priorities.</td></tr>
<tr><td>...</td><td>...</td></tr>
</table>
https://docs.trendmicro.com/en-us/enterprise/trend-micro-apex-central-2019-online-help/introduction/introducing-control-/whats-new-in-this-ve.aspx

"<b>Intrusion Prevention Rules</b>

The <b>Intrusion Prevention Rules</b> screen displays the Intrusion Prevention Rules supported by Apex Central Vulnerability Protection. Intrusion Prevention Rules examine the actual content of network packets (and sequences of packets). Based on the conditions set within the Intrusion Prevention Rule, various actions are then carried out on these packets. These actions include replacing specifically defined or suspicious byte sequences, or completely dropping packets and resetting the connection.

• To filter the list of rules, use the Search box to specify full or partial strings that appear in any of the columns.
• To sort the list of Intrusion Prevention Rules by column data, click a column heading.
• To view detailed Intrusion Prevention Rule Properties, click the link in the Name column of a rule."
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 14-33 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)
</td></tr>
</table>

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td>
"The Threat Type column displays the following threat types.
<table>
<tr><th>Threat Type</th><th>Description</th></tr>
<tr><td>Ransomware</td><td>Malware that prevents or limits users from accessing their system unless a ransom is paid</td></tr>
<tr><td>Known Advanced Persistent Threat (APT)</td><td>Intrusions by attackers that aggressively pursue and compromise chosen targets, often conducted in campaigns—a series of failed and successful attempts over time to get deeper and deeper into a target network—and not isolated incidents</td></tr>
<tr><td>Social engineering attack</td><td>Malware or hacker attacks that exploits a security vulnerability found in documents, such as a PDF file</td></tr>
<tr><td>Vulnerability attack</td><td>Malware or hacker attacks that exploits a security weakness typically found in programs and operating systems</td></tr>
<tr><td>Lateral movement</td><td>Searches for directories, email, and administration servers, and other assets to map the internal structure of a network, obtain credentials to access these systems, and allow the attacker to move from system to system</td></tr>
<tr><td>Unknown threats</td><td>Suspicious objects (IP addresses, domains, file SHA-1 hash values, email</td></tr>
</table>
</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

<table>
<tr><th>Claim 14 Elements</th><th>Applicability</th></tr>
<tr><td></td><td><table><tr><td></td><td>messages) with the "high" risk level, as detected by Deep Discovery Inspector, endpoint security products, or other products with Virtual Analyzer</td></tr><tr><td>C&C callback</td><td>Attempts to communicate with a command-and-control (C&C) server to deliver information, receive instructions, and download other malware</td></tr></table><i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-20 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)</td></tr>
<tr><td>wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is identified based on an identification of an operating system.</td><td>Trend Micro Apex Central includes <i>wherein the computer program product is operable such that one or more of the plurality of mitigation techniques</i> (e.g., threat analysis and/or outbreak control, etc.) <i>is identified based on an identification of an operating system</i> (e.g., a Windows, Mac, Linux, and/or Android operating system, etc.).

"<b>Vulnerability attack</b>

Malware or hacker attacks that <u>exploits a security weakness typically found in programs and operating systems</u> (pg 3-10)"
<i>Trend Micro Apex Central Administrator's Guide</i>, Version: 2019, Page 3-10 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)

"Procedure
1. Go to <b>Administration > Security Agent Download</b>.
2. Select the operating system.</td></tr>
</table>

Patent No. 9,100,431, Claim 14: Trend Micro's Apex Central

Claim 14 Elements	Applicability
	• **Windows 64-bit**: Select to create a 64-bit MSI installation package for Apex One Security Agents • **Windows 32-bit**: Select to create a 32-bit MSI installation package for Apex One Security Agents • **Mac OS**: Select to create a ZIP installation package for Apex One (Mac) Security Agents" *Trend Micro Apex Central Administrator's Guide*, Version: 2019, Page 9-3 (https://docs.trendmicro.com/all/ent/apex-cen/2019/en-us/apexCen_2019_ag.pdf)